APPLICATIONS OF P-ADIC NUMBERS

By

WILLIAM AARON LETIZIA

A Thesis Submitted to The Honors College

In Partial Fulfillment of the Bachelors degree
With Honors in

Mathematics

THE UNIVERSITY OF ARIZONA

M A Y 2 0 1 9

Approved by:

_____
Professor Bryden Cais
Department of Mathematics

1 Abstract

The p-adic numbers give a new technique to answer questions about the integers and rational numbers. While they are typically used in a more abstract setting, I will present two concrete applications of p-adic numbers. The major results that I will prove in this paper are that any finite subgroup of $GL_n(\mathbb{Q})$ must divide 24 and that the set of zeros of any integer linear recurrence sequence is the union of a finite number of finite sets and a finite number of arithmetic progressions. The latter result is better known as the Skolem-Mahler-Lech Theorem.

2 Acknowledgments

The genesis of this paper was an Honors Independent Study on p-adic numbers supervised by Jeremy Booher. We are grateful for his immense influence and unwavering support.

3 Finite Subgroups of $GL_n(\mathbb{Q})$

At first glance, it may not be entirely clear if the finite subgroups of $GL_n(\mathbb{Q})$ can be bound or how we can use p-adic numbers to say anything about them. In this section, we will explore how to answer questions about $GL_n(\mathbb{Q})$ using $GL_n(\mathbb{Z}_p)$.

Lemma 1. *Suppose that $p > 2$ is prime. If $A \in GL_n(\mathbb{Z}_p)$ satisfies $A \equiv I_n \bmod p$ and A has finite order, then $A = I_n$.*

Proof. Without loss of generality, assume $|A| = q$, q a prime. Then $A = I_n + p^l B$ where $B \in M_{n\times n}(\mathbb{Z}_p)$ with some entry of B is not a multiple of p and $l \geq 1$. While the binomial theorem does not hold for matrices in general due to lack of commutativity, we can use it in this case since I_n commutes with any other matrix. By applying the binomial theorem, we

get that

$$\begin{aligned} I_n &= A^q \\ &= (I_n + p^l B)^q \\ &= \sum_{k=0}^{q} \binom{q}{k} (I_n)^{q-k} (p^l B)^k \\ &= I_n + \sum_{k=1}^{q} \binom{q}{k} p^{kl} B^k \end{aligned}$$

which implies that

$$\begin{aligned} 0 &= \sum_{k=1}^{q} \binom{q}{k} p^{kl} B^k \\ &= qp^l B + \sum_{k=2}^{q} \binom{q}{k} p^{kl} B^k. \end{aligned}$$

First, consider the case where $p \nmid q$. Notice that $\upsilon_p(qp^l B) = l$, but $\upsilon_p\left(-\sum_{k=2}^{q} \binom{q}{k} p^{kl} B^k\right) > l$. This implies that $B = 0$ must be true for the equality, $qp^l B = -\sum_{k=2}^{q} \binom{q}{k} p^{kl} B^k$, to hold.

Now, consider the case p = q. Now the binomial coefficient may contribute or take away powers of p. But we have that

$$\begin{aligned} \upsilon_p\left(\binom{p}{k}\right) &\geq 1 - \left\lfloor \frac{k}{p} \right\rfloor \\ &= 1 \end{aligned}$$

for $1 \leq k \leq p-1$. So then, again, we have that $\upsilon_p(p^{l+1}B) = l+1$ but $\upsilon_p\left(-\sum_{k=2}^{q} \binom{q}{k} p^{kl} B^k\right) > l+1$. Thus, $B = 0$.

Therefore, in both cases, we have that if $A \equiv I_n \bmod p$ and A has finite order, then $A = I_n$. □

Lemma 2. *$GL_n(\mathbb{F}_p)$ has order*

$$\prod_{i=0}^{n-1} (p^n - p^i) = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$$

Proof. Suppose $A \in GL_n(\mathbb{F}_p)$. Since an $n \times n$ matrix is invertible if and only if its columns are linearly independent, we have $p^n - 1$ choices for the first column, i.e., any choice of elements in $\mathbb{F}_p$ suffice as long as they're not all 0.

Then, given the first column, the second column must be linearly independent to the first, i.e., if $\mathbf{a}_1$ is the first column, $\mathbf{a}_2 \neq m \cdot \mathbf{a}_1$ for some $m \in \mathbb{F}_p$. This means, given choice of first column, there are $p^n - p$ choices for the second column.

Similarly, $\mathbf{a}_3 \neq m_1 \cdot \mathbf{a}_1 + m_2 \cdot \mathbf{a}_2$ for some $m_1, m_2 \in \mathbb{F}_p$. That is, $\mathbf{a}_3 \notin \text{Span}\{\mathbf{a}_1, \mathbf{a}_2\}$. Thus, given choice of first and second columns, there are $p^n - p^2$ choices for the third column.

We continue by induction to conclude that there are $\prod_{i=0}^{n-1}(p^n - p^i)$ invertible matrices in $M_{n\times n}(\mathbb{F}_p)$, and thus the order of $GL_n(\mathbb{F}_p)$ is $\prod_{i=0}^{n-1}(p^n - p^i)$. □

Corollary 3. *If G is a finite subgroup of $GL_n(\mathbb{Z}_p)$, then*

$$\#G | \prod_{i=0}^{n-1}(p^n - p^i)$$

Proof. Let G be a finite subgroup and consider the projection map $\pi : G \twoheadrightarrow GL_n(\mathbb{F}_p)$. Consider an element $A \in \ker(\pi)$. Since G is finite, A has finite order and $A \equiv I_n \pmod{p}$. By Lemma 1, we have that $A = I_n$, that is, $\ker(\pi) = \{I_n\}$. By the First Isomorphism Theorem, $G \cong \text{im}(\pi)$. Since any subgroup of $GL_n(\mathbb{F}_p)$ has order dividing $\prod_{i=0}^{n-1}(p^n - p^i)$ by Lemma 2 and Lagrange's Theorem, we have that $\#G \mid \prod_{i=0}^{n-1}(p^n - p^i)$. □

Using this information we have about $GL_n(\mathbb{Z}_p)$ for a fixed by arbitrary prime p, we can make global statements about elements in $GL_n(\mathbb{Z})$. Next, we will want to deduce facts about the order of G when considered as a subgroup of $GL_n(\mathbb{Q})$. I claim that we can answer these questions for $GL_n(\mathbb{Z})$ and it will hold for $GL_n(\mathbb{Q})$. I will not prove this here, but I will cite Keith Conrad's paper that has an argument for it [Con].

Additionally, I will state the following as a fact and prove the case only for odd primes. For the necessary alteration to the odd prime proof, I also recommend looking at Keith

Conrad's paper for a more complete treatment [Con].

Fact 4. *If G is a finite subgroup of $GL_n(\mathbb{Q})$, then*

$$v_2(\#G) = b_2 = n + \sum_{i=1}^{\infty} \left\lfloor \frac{n}{2^i} \right\rfloor$$

Theorem 5. *If G is a finite subgroup of $GL_n(\mathbb{Q})$, then*

$$\#G \mid \prod_q q^{b_q}$$

where, for q an odd prime,

$$b_q = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{q^i(q-1)} \right\rfloor$$

and where

$$b_2 = n + \sum_{i=1}^{\infty} \left\lfloor \frac{n}{2^i} \right\rfloor$$

Proof. Given a prime q and a fixed n, we want to find a prime p such that it divides $\prod_{k=0}^{n-1}(p^n - p^k)$ minimally. That is, we want to find a prime p that is congruent (mod q^i) to a generator of $(\mathbb{Z}/q^i\mathbb{Z})^\times$ for each $i \in \mathbb{Z}_+$. By Dirichlet's Theorem [Ser73, Theorem VI.4.1.2], if a and q^i are relatively prime, then there are infinitely many primes p such that $p = kq^i + a$. This means that we can always find a prime p such that $p \equiv a \pmod{q^i}$ where a is a generator of $(\mathbb{Z}/q^i\mathbb{Z})^\times$.

The end goal is to find an upper bound on how many times each q^i divides $\prod_{k=0}^{n-1}(p^n - p^k)$. Let's start first with $q^1 = q$. Choose a prime p_1 such that $p_1 \equiv a_1 \pmod{q}$, a_1 a generator of $(\mathbb{Z}/q\mathbb{Z})^\times$. Then, by Fermat's Little Theorem, we get that $p_1^{q-1} \equiv 1 \pmod{q}$. This is also true for each power that is a multiple of $q-1$, i.e., $p_1^{m(q-1)} \equiv 1 \pmod{q}$ for some $m \in \mathbb{Z}_+$. So for q, we count the number of multiples of $q-1$ are less than n, that is, so far we have that $b_q \geq \left\lfloor \frac{n}{q-1} \right\rfloor$.

We do a similar counting for each q^i. I will describe this counting again for q^i, $i \in \mathbb{Z}_+$.

From Gauss and elementary modern algebra we have that $(\mathbb{Z}/q^i\mathbb{Z})^\times \cong (\mathbb{Z}/(q^{i-1}(q-1))\mathbb{Z})$. So $(\mathbb{Z}/q^i\mathbb{Z})^\times$ is cyclic. So now we find a generator, a_i, for $(\mathbb{Z}/q^i\mathbb{Z})^\times$ and a prime, p_i, such that $p_i \equiv a_i \pmod{q^i}$. Again, due to Fermat's Little Theorem, we have that $p_i^{mq^{i-1}q-1} \equiv 1$ for each $m \in \mathbb{Z}_+$. Since the number of $p^j - 1$ divisible by q^i is equal to the number of multiples of $q^{i-1}(q-1)$ less than n, we have that there are $\left\lfloor \frac{n}{q^{i-1}(q-1)} \right\rfloor$ times that q^i divides $p^j - 1$.

Adding up these counts for each nonnegative integer power gives us the b_q we're after:

$$b_q = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{q^i(q-1)} \right\rfloor$$

Then, combining this with the fact we used for $q = 2$, we get

$$\#G | \prod_q q^{b_q}$$

as desired. □

Now, let's specialize a bit–let $n = 2$ and consider finite subgroups of $GL_2(\mathbb{Q})$.

Example 6. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ and let $G = \langle A \rangle$. Then $\#G = 6$.

Example 7. Let $X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and let $Y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and let $G = \langle X, Y \rangle$. Notice that, if we think of these matrices acting on vectors in $\mathbb{R}^2$, then $X\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $X\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, $Y\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $Y\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$. This shows that X corresponds to a rotation by $\frac{\pi}{2}$ and Y corresponds to a reflection across the y-axis. That means this group is isomorphic to D_8, and so $\#G = 8$. This example comes from [Con, Example 8].

Corollary 8. *If $G \subset GL_2(\mathbb{Q})$ is a finite subgroup, then $\#G | 24$.*

Proof. Let $n = 2$. Then by plugging into the equation from Theorem 5, we have that

$$\begin{aligned} b_2 &= n + \left\lfloor \frac{n}{2} \right\rfloor + \sum_{i=2}^{\infty} \left\lfloor \frac{n}{2^i} \right\rfloor \\ &= 2 + \left\lfloor \frac{2}{2} \right\rfloor + \sum_{i=2}^{\infty} \left\lfloor \frac{2}{2^i} \right\rfloor \\ &= 3 \end{aligned}$$

and

$$\begin{aligned} b_3 &= \sum_{i=0}^{\infty} \left\lfloor \frac{n}{3^i(3-1)} \right\rfloor \\ &= \left\lfloor \frac{n}{3-1} \right\rfloor + \sum_{i=1}^{\infty} \left\lfloor \frac{n}{3^i(3-1)} \right\rfloor \\ &= \left\lfloor \frac{2}{3-1} \right\rfloor + \sum_{i=1}^{\infty} \left\lfloor \frac{2}{3^i(3-1)} \right\rfloor \\ &= 1. \end{aligned}$$

For all primes q, $q > 3$, we have that

$$\begin{aligned} b_q &= \sum_{i=0}^{\infty} \left\lfloor \frac{n}{q^i(q-1)} \right\rfloor \\ &= \sum_{i=0}^{\infty} \left\lfloor \frac{2}{q^i(q-1)} \right\rfloor \\ &= 0 \end{aligned}$$

Then we get that

$$\begin{aligned} \prod_q q^{b_q} &= 2^3 \cdot 3^1 \cdot \prod_{q \geq 5} q^0 \\ &= 24 \end{aligned}$$

Therefore, $\#G \mid 24$. □

4 Linear Recurrence Sequences and the Skolem-Mahler-Lech Theorem

Definition 9. A **linear recurrence sequence** is a sequence of numbers $(a_n)_{n=0}^{\infty}$ satisfying an equation

$$a_n = \sum_{i=1}^{d} c_i a_{n-i} = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_d a_{n-d}$$

for all $n \geq d$, where c_j and a_k are fixed numbers for $1 \leq j \leq d$ and $0 \leq k \leq d-1$.

An **integer linear recurrence sequence** is a linear recurrence sequence where each a_i and c_i is an integer.

Example 10. Possibly the most well-known integer linear recurrence sequence is the Fibonacci sequence, $1, 1, 2, 3, 5, 8, 13, 21, \ldots$. Formally, we can express the Fibonacci sequence as:

$$a_n = a_{n-1} + a_{n-2} \text{ with } a_0 = 1 \text{ and } a_1 = 1$$

Notice that this sequence starts at 1 and always increases after the second entry. In other words, this sequence is never zero.

Example 11. As a small variant, here's what I call the "computer scientist's Fibonacci sequence,"

$$a_n = a_{n-1} + a_{n-2} \text{ with } a_0 = 0 \text{ and } a_1 = 1.$$

This sequence is essentially the regular Fibonacci sequence, but "shifted over" one place so that it starts at 0. So it looks like $0, 1, 1, 2, 3, 5, 8, 13, \ldots$. As with the reasoning in the previous example, this sequence has only one zero, its first entry.

Example 12. Another simple example of a integer linear recurrence sequence is:

$$a_n = a_{n-2} \text{ with } a_0 = 0 \text{ and } a_1 = 1$$

This sequence is $0, 1, 0, 1, 0, 1, ...$, that is, the sequence where each even-indexed element is 0 and each odd-indexed element is 1. So this sequence contains an infinite number of zeros.

With these examples in mind, it's natural to think, "In what ways can the zeros of an integer linear recurrence sequence appear?" This question is answered by the Skolem-Mahler-Lech Theorem.

Theorem 13. *(Skolem). Let* $\mathbf{a} = (a_n)_{n=0}^{\infty}$ *be an integer linear recurrence sequence. Then the set of zeros of* $\mathbf{a}$*,* $Z(\mathbf{a})$*, is the union of a finite set and a finite list of arithmetic progressions.*

From the Fibonacci sequence, it's clear that the finite set and the finite list of arithmetic progressions could be empty. This result was originally proven in this form by Skolem in 1934, but it was extended to number fields by Mahler in 1935 and then further extended to arbitrary fields of characteristic zero by Lech in 1952, see [Fra] for the history.

We'll prove this result following the strategies outlined in [Fra] and [Lit].

First, let $\mathbf{a}$ be an integer linear recurrence sequence satisfying

$$a_n = \sum_{i=1}^{d} c_i a_{n-i}$$

for all $n \geq d$. Without loss of generality, assume $c_d \neq 0$ (for, if it is, then we can use a smaller d). Define the following matrices:

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_d & c_{d-1} & c_{d-2} & \cdots & c_1 \end{pmatrix}, \; v = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{pmatrix}, \; e = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Then we have that $\langle A^n v, e\rangle = a_n$ for all $n \geq 0$. Indeed, the product $A^n v = \begin{pmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+d-1} \end{pmatrix}$ and the inner product with the vector $e = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ gives us the first entry of $A^n v$, a_n.

By considering linear independence of the columns of A, it is clear that A is invertible if and only if $c_d \neq 0$. Choose a prime p that does not divide $\det(A)$, that is, a prime p such that A is invertible mod p. Reduce all of the entries of A modulo p. Since $GL_d(\mathbb{F}_p)$ is finite in size, there exists an $m \in \mathbb{Z}_+$ such that $A^m \equiv I_d \pmod{p}$.

First, we define a family of sets that will be useful to us in the proof of Skolem-Mahler-Lech.

Definition 14. Given $m \in \mathbb{Z}_+$, define the set

$$S_r = \{n \in \mathbb{N} : a_{mn+r} = 0\}$$

for each $0 \leq r \leq m-1$.

Next, since we can embed $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, we will build up some machinery about p-adic analysis and p-adic analytic functions needed to prove the Skolem-Mahler-Lech Theorem.

Definition 15. Let B be an open ball in $\mathbb{Z}_p$. A function $f : B \to \mathbb{Z}_p$ is p-adic analytic if it is equal to a power series

$$f(z) = \sum_{k \geq 0} a_k (z - b_0)^k$$

for some $b_0 \in B$ which converges for all $z \in B$.

We will use the fact that $\mathbb{Z}_p$ is compact, proven in [Gou97] and [Lit]. Specifically, we will

use that that $\mathbb{Z}_p$ is limit point compact (i.e., every infinite subset of $\mathbb{Z}_p$ has a limit point). We refer the reader to [Gou97, Chapter 4] for the details about p-adic analysis used in this proof.

Theorem 16. *(Strassmann). Let $f : B \to \mathbb{Z}_p$ be a p-adic analytic function. Then either f is identically zero or has only finitely many zeros in B.*

Proof. Suppose f has infinitely many zeros, say $f(b_k) = 0$. Then, since $\mathbb{Z}_p$ is compact, the b_k have a limit point b. Expand f about b to get

$$f(z) = \sum a_k (z-b)^k.$$

If f is not identically zero, there exists an $a_k \neq 0$. Let a_N be the first such coefficient. Then

$$f(z) = (z-b)^N (a_N + (z-b)g(z)).$$

Since the image of a closed ball, which is compact in $\mathbb{Z}_p$), is compact, we have that $|g(z)|_p$ must be bounded above. Then we have, for $|z-b|_p$ sufficiently small,

$$|(z-b)g(z)|_p < |a_N|_p.$$

That is, f is non-zero on a small punctured disk about b. But this contradicts that b was a limit point of the b_k. Thus, if f has infinitely many zeros, then f is identically zero. □

Lemma 17. *For each $0 \leq r \leq m-1$, $S_r = \{n \in \mathbb{N} : a_{mn+r} = 0\}$ is either finite or all of $\mathbb{N}$.*

Proof. Fix m, $r \in \mathbb{Z}$ and assume S_r is infinite. If we show that $S_r = \mathbb{N}$, we're done. Define a function $P_r : \mathbb{Z} \to \mathbb{Z}_p$ by

$$P_r(n) = a_{mn+r} = \langle (I_d + pB)^n A^r v, e \rangle$$

where B is a $d \times d$ matrix of integers such that $A^m = I_d + pB$. Then $P_r(n)$ is a subsequence

of $\mathbf{a}$ and S_r is its zero set. As in the previous section, since I_d commutes with any matrix, we may use the binomial theorem on $(I_d + pB)^n$. By doing so, we get

$$(I_d + pB)^n = \sum_{i=0}^{n} \binom{n}{i} p^i B^i.$$

Then, if we define $f_i(n) = \left\langle \binom{n}{i} B^i A^r v, e \right\rangle \in \mathbb{Z}[n]$, we get

$$P_r(n) = \sum_{i=0}^{\infty} p^i f_i(n)$$

which is convergent as a p-adic analytic function on the closed ball $\mathbb{Z}_p$. If we think of P_r as a sequence of points in $\mathbb{Z}_p$, since P_r is a p-adic analytic function, we can apply Strassmann's Theorem to P_r to conclude, since we assumed S_r is infinite, that $S_r = \mathbb{N}$. □

Now we will prove Skolem's theorem.

Proof of Skolem. To summarize, $\mathbf{a} = (a_n)_{n=0}^{\infty} = \bigcup_{r=0}^{m-1} P_r$ and from Lemma 17 we have that S_r is finite or all of $\mathbb{N}$ for each $0 \leq r \leq m-1$. If $S_r = \mathbb{N}$, that means that the arithmetic progression $mn + r$ of indices (corresponding to $P_r(n) = (a_{mn+r})_{n=0}^{\infty}$) are zeros. That is, $Z(\mathbf{a}) = \bigcup_{r=0}^{m-1} S_r$ is the union of a finite number of finite sets and a finite number of arithmetic progressions, as desired. □

References

[Con] Keith Conrad, *Prime powers units and finite subgroups of $gl_n(\mathbb{Q})$*, [Online; accessed 9-May-2018].

[Fra] Cameron Franc, *The theorem of skolem-mahler-lech*, [Online; accessed 9-May-2018].

[Gou97] Fernando Q. Gouvêa, *p-adic numbers*, second ed., Universitext, Springer-Verlag, Berlin, 1997, An introduction. MR 1488696

[Lit] Daniel Litt, *Zeroes of integer linear recurrences*, [Online; accessed 9-May-2018].

[Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7. MR 0344216